High Confidence Medical Device Software Systems

The area of Cyber Physical Systems (CPS) – that is, NIT systems connecting with the physical world needs to be the highest priority among the eight technical priority areas recommend by the PCAST report. This is necessary to maintain American Competitiveness, as CPS is where other countries EU and Asian countries are aggressively investing in their R&D programs. The application domains of CPS include healthcare, transportation, process control and energy distribution, large-scale physical infrastructures, and defense systems.

Given the shortage of caregivers and the growth of an aging US population, the future of US healthcare quality does not look promising and definitely is unlikely to be cheaper. Advances in healthcare technology and health information systems offer a tremendous opportunity for improving the quality of our healthcare while reducing healthcare costs [1].

The development and production of medical device software and systems is a crucial issue, both for the US economy and for ensuring safe advances in healthcare delivery. As devices become increasingly smaller in physical terms, but larger in software terms, the design, testing, and eventual Food and Drug Administration (FDA) device approval is becoming much more expensive for medical device manufacturers both in terms of time and cost. Furthermore, the number of devices that have recently been recalled due to software and hardware problems is increasing at an alarming rate. As medical devices are becoming increasingly networked, ensuring even the same level of health safety seems a challenge [2].

The cross-cutting nature of medical device design—transcending the informational, physical, and medical worlds—along with the possibility of a nationwide networked medical system that actively monitors and regulates the health of our nation's citizens, raises immense scientific and technological R&D challenges for the IT, medical, and regulatory communities. The challenges envisioned for the next five to ten years include the following:

- System integration. As we embrace a plug-and-play vision of medical device networks in future digital hospitals and digital homes, we must collectively facilitate the development of medical device systems and coordinate them with the development of standards for the architecture and communication of interoperable plug-and-play device networks. Achieving these goals while establishing quality-of-service levels that ensure system and patient safety on the one hand, and patient security and privacy on the other, is a great challenge.

- Critical infrastructure. As we move toward an environment in which all patients are constantly monitored and actively plugged into a nationwide medical information network, we are creating a new critical infrastructure that will literally monitor the nation's health. We need new methods to ensure the safety and security of that network, particularly methods involving the active use of information for medical purposes. In the presence of abnormal conditions or attacks, the system's performance must degrade gracefully and safely, and the system must identify, contain, and, if possible, repair faults while providing timely notification to human operators.

- Embedded real-time systems design. Medical devices are embedded not only inside information networks but also inside human patients, whose critical life-functions they monitor and regulate. The design of medical devices is therefore more than an NIT issue; it must also include the device's interaction with the patient and the environment and the context in which they coexist. Thus, we need a fundamental rethinking of medical device design—toward a holistic approach that integrates functional, computational, and communication designs in the presence of highly uncertain patient models in both normal and abnormal conditions.

- Verification, validation and certification. Current design practice makes certification and verification an afterthought, taking place at the end of the design cycle, when it is frequently too late to change design choices. As medical devices become more complex and more interconnected, it is becoming increasingly evident that certification should be incorporated in early design stages. Furthermore, certification and design frameworks are currently not component-based, resulting in time-consuming and expensive certification of large integrated systems. This drawback makes the current approach inefficient for certification of incremental or evolutionary designs, and creates difficulties in maintaining or upgrading legacy systems.

To address these challenging R&D issues, there must be coordination among funding agencies (NSF, NIH, DoD), the regulating and standardization agencies (FDA, NIST). Such coordination activities should promote collaborations between academic researchers and medical device manufacturers. There then lies the potential to create a new scientific community and a new generation of scientists and engineers that integrate computer science, engineering, and medicine.

References

[1] Insup Lee, George Pappas, Rance Cleaveland, John Hatcliff, Bruce Krogh, Peter Lee, Harvey Rubin, Lui Sha, "High-Confidence Medical Device Software and Systems," IEEE Computer, vol 39, no 4, April 2006. pp. 33-38.

[2] Proceedings of Joint HCMDSS/MD PnP workshop, Julian Goldman, Insup Lee, Oleg Sokolsky, Susan Whitehead, Eds., IEEE Press, June 25-27, 2006. (www.cis.upenn.edu/hcmdss07/)